Emri: _____ Data: _____ Pikët: _____

Bazat e sigurisë kibernetike dhe kërcënimet online Parandalimi

Kërcënimet e sigurisë kibernetike, firewall-et e rrjetit, autentikimi me shumë faktorë, kuadrot e sigurisë

PËRMBLEDHJE MËSIMORE PËR BAZAT E SIGURISË KIBERNETIKE

I SIGURUAR
ENKRIPTIMI I TË DHËNAVE
Standardi AES 256-bit

I PËRPUTHSHËM
STANDARDET GLOBALE
Kornizat GDPR dhe CCPA

ZERO-TRUST
POLITIKA E QASJES
Autentikim me shumë faktorë

Mirë se vjen! Kjo paketë aktivitetesh të udhëheq përmes parimeve themelore të bazave të sigurisë kibernetike dhe parandalimit të kërcënimeve në internet. Do të eksplorosh kërcënimet e malware-it, autentikimin me shumë faktorë, firewall-et e rrjetit dhe kuadrot e reagimit ndaj incidenteve.

PIKAT E KONTROLLIT TË FLETËS SË PUNËS

- [ ] **Pjesët 1-4: Zotëro sigurinë kibernetike dhe parandalimin e kërcënimeve.**
- [ ] **Pjesët 5-7: Zgjidh fjalëkryqe dhe enigma me kërkim fjalësh.**
- [ ] **Pjesët 8-9: Zgjidh studime rasti dhe sfidën e kodit.**
- [ ] **Pjesa 10: Shqyrto faqet e pyetjeve të shpeshta bazë dhe të avancuara.**
- [ ] **Pjesa 11: Eksploro 10 fakte interesante nga bota reale.**
- [ ] **Bonus: sfida Mendo shpejt.**

Hap Udhëzuesin VPN.com për sigurinë kibernetike

URL: https://www.vpn.com/sq/siguria-kibernetike/

Udhërrëfyesi yt mësimor për bazat e sigurisë kibernetike

- Identifiko vektorët e zakonshëm të malware-it, phishing-ut dhe të ndërhyrjes në rrjetin e korporatës.
- Zbato kontrolle standarde të sigurisë kibernetike, përfshirë MFA, firewall-et dhe mbrojtjen e pikave fundore.
- Vlerëso procedurat e reagimit ndaj incidenteve për zbutjen e ndikimit të shkeljeve të të dhënave.
- Analizo faktorët e rrezikut organizativ dhe përafrimin e sigurisë sipas udhëzimeve të NIST.
- Konfiguro praktikat e higjienës së sigurisë për të zbutur credential stuffing-un e automatizuar.

UDHËZIME PËR UDHËZUESIN E SIGURISË KIBERNETIKE

Përgjigju pyetjeve me zgjedhje të shumëfishtë dhe pyetjeve E vërtetë/E gabuar, plotëso fjalitë me vende bosh duke përdorur bankën e fjalëve, përputh përkufizimet dhe zgjidh fjalëkryqin dhe enigmën e kërkimit të fjalëve. Zbato njohuritë e tua për parandalimin e kërcënimeve. Përfundo me aktivitetin bonus Mendo shpejt.

BAZAT E SIGURISË KIBERNETIKE DHE PARANDALIMI I KËRCËNIMEVE (HYRJE)

Siguria kibernetike mbron rrjetet, sistemet dhe të dhënat nga sulmet dixhitale të paautorizuara. Zhvillimi i zakoneve të forta të sigurisë, konfigurimi i firewall-eve, kërkesa e autentikimit me shumë faktorë dhe trajnimi i stafit për njohjen e kërcënimeve janë përbërës thelbësorë të mbrojtjes së rrjetit të korporatës.

LEXO ÇDO PIKË KONTROLLI ME KUJDES DHE ZGJIDH OSE SHKRUAJ PËRGJIGJEN E SAKTË.

Pika e kontrollit 1: Sfida me zgjedhje të shumëfishtë

1 **1. Cili është objektivi kryesor i një sulmi phishing?**

- A. Vjedhja e kredencialeve dhe e të dhënave të ndjeshme të përdoruesit
- B. Rritja e dukshmërisë së faqes në motorët e kërkimit
- C. Rritja e kapacitetit të gjerësisë së brezit të rrjetit
- D. Menaxhimi i replikimit të qendrës rezervë të të dhënave

2 **2. Cili mekanizëm ofron mbrojtjen më të fortë të llogarisë?**

- A. Autentikim shumëfaktorësh me çelësa harduerikë
- B. Fjalëkalime komplekse të përditësuara çdo tridhjetë ditë
- C. Kufizimi i hyrjes në llogari vetëm në orët e punës
- D. Fshehja e emrit të përdoruesit të llogarisë nga drejtoritë publike

3 **3. Çfarë e përcakton ngarkesën e infektimit me ransomware?**

- A. Enkriptimi i skedarëve të sistemit dhe kërkesa për pagesë
- B. Regjistrimi i fshehtë i goditjeve të tastierës në serverë të largët
- C. Injektimi i reklamave të paautorizuara në shfletues
- D. Përdorimi i burimeve lokale të CPU-së për të minuar kriptovalutë

4 **4. Si ndikon një exploit zero-day në mbrojtjet e sigurisë?**

- A. Synon cenueshmëri të papatch-uara dhe të panjohura
- B. Çaktivizon automatikisht firewall-in e korporatës
- C. E detyron sistemin të bëjë një rindezje të plotë
- D. Nuk kërkon buxhet për t'u riparuar

5 **5. Cili kuadër rregullon kontrollet e sigurisë së kompanisë?**

- A. Udhëzimet e NIST Cybersecurity Framework
- B. Specifikimet e skemës së dokumentit W3C HTML5
- C. Manualet e instalimit të drajverëve të printerit
- D. Përkufizimet e protokolleve të rutimit IETF

Pika e kontrollit 2: Sfida: E vërtetë ose e gabuar

6 Pyetje E/G 6

6. Sulmet phishing synojnë vetëm llogaritë personale të email-it.

○ E vërtetë ○ E gabuar

7 Pyetje E/G 7

7. Autentikimi me shumë faktorë ndihmon në bllokimin e sulmeve credential stuffing.

○ E vërtetë ○ E gabuar

8 Pyetje E/G 8

8. Firewall-et inspektojnë trafikun e rrjetit për të bllokuar qasjen e paautorizuar në porta.

○ E vërtetë ○ E gabuar

9 Pyetje E/G 9

9. Korrigjimi i shfrytëzimeve zero-day kërkon përditësime standarde të përkufizimeve të antivirusit.

○ E vërtetë ○ E gabuar

10 Pyetje E/G 10

10. Një honeypot është një server karth që përdoret për të joshur kriminelët kibernetikë.

○ E vërtetë ○ E gabuar

Pika e kontrollit 3: Futja e termave kryesorë

Lexo secilën fjali më poshtë dhe plotëso vendin bosh me termin e saktë nga Banka e Fjalëve.

1. Administratorët e rrjetit instalojnë një _____ për të filtruar trafikun hyrës.

2. Një sulmues përdor një _____ zero-day për të anashkaluar arnimet e sistemit.

3. Sulmuesit dërgojnë email-e të falsifikuara për të kryer fushata _____ kundër punonjësve.

4. Ransomware është një formë shkatërruese e _____ që bllokon të dhënat e përdoruesit.

5. Një _____ e fortë e fjalëkalimeve zbut rreziqet e vjedhjes së kredencialeve.

6. Për të mbrojtur komunikimet e ndjeshme, përdoruesit zbatojnë protokolle të bazuara në: _____ .

BANKA E FJALËVE TË LEKSIKUT

EKSPLOIT ENKRIPTIM FIREWALL HIGJIENË HONEYPOT MALWARE MULTIFAKTORIAL PHISHING

Shkruaj përgjigjet e tua këtu:

1.
2.
3.
4.
5.
6.

Pika e kontrollit 4: Përputhja e koncepteve të sigurisë

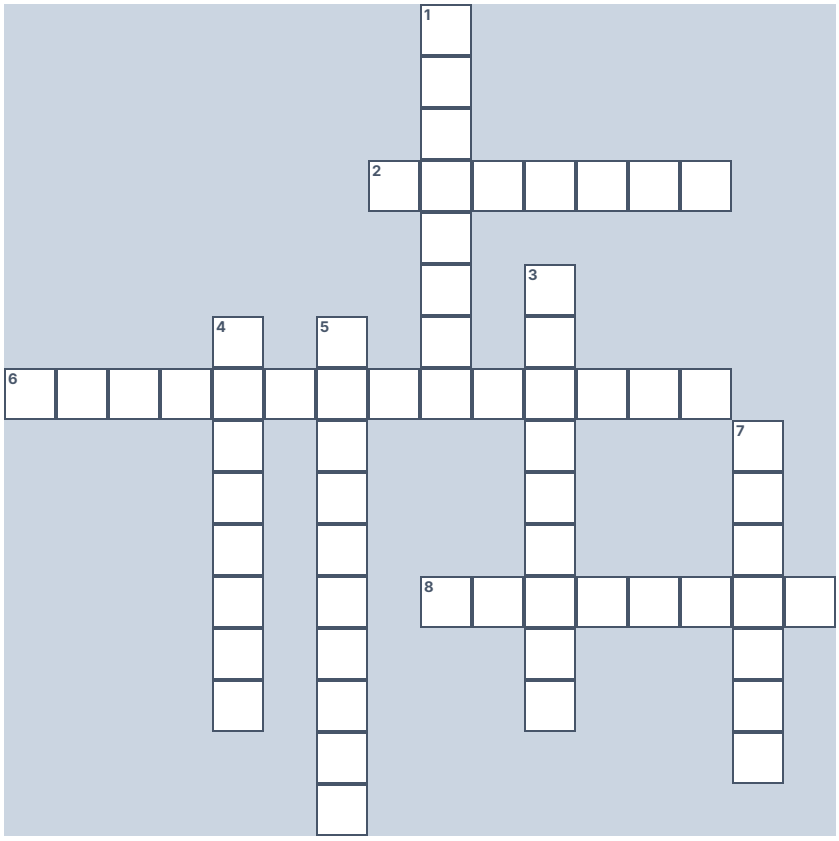
PËRPUTHJA E PËRKUFIZIMEVE

Përputh çdo term fjalori në të majtë me përkufizimin e tij të saktë në të djathtë, duke shkruar shkronjën përkatëse (A-H) në kutinë e plotësueshme.

☐	1. Kërcënimi i ransomware-it	A	Udhëzime të strukturuara si NIST që përdoren për të menaxhuar rreziqet kibernetike.
☐	2. Autentikim shumëfaktorësh	B	Plan i strukturuar për trajtimin dhe zbutjen e cenimeve të sigurisë.
☐	3. Shfrytëzim zero-day	C	Barrierë rrjeti që filtron trafikun sipas rregullave të sigurisë.
☐	4. Honeypot joshës	D	Malware që enkripton të dhënat dhe kërkon pagesë financiare për deshifrim.
☐	5. Firewall kundër ndërhyrjeve	E	Shfrytëzim i një cenueshmërie i synuar para se furnizuesi të publikojë një arnim.
☐	6. Reagimi ndaj incidenteve	F	Praktikat më të mira për menaxhimin e kredencialeve dhe çelësave të vërtetimit.
☐	7. Higjiena e fjalëkalimeve	G	Validim sigurie që kërkon dy ose më shumë faktorë autentikimi.
☐	8. Kornizë sigurie	H	Sistem joshës i ngritur për të tërhequr dhe analizuar aktorët keqdashës.

Pika e kontrollit 5: Fjalëkryq

Zgjidhe fjalëkryqin duke shkruar shkronja në kutitë e bardha aktive. Numrat korrespondojnë me indiciet më poshtë.



HORIZONTALISHT

2. Eksploit i synuar para se shitësi të lëshojë një arnim (7)

6. Verifikim sigurie që kërkon dy ose më shumë faktorë autentikimi (14)

8. Praktikat më të mira për menaxhimin e kredencialeve dhe çelësave të autentikimit (8)

VERTIKALISHT

1. Sistem joshës i ngritur për të joshur dhe analizuar aktorët keqdashës (8)

3. Plan i strukturuar për trajtimin dhe zbutjen e shkeljeve të sigurisë (9)

4. Barrierë rrjeti që filtron trafikun sipas rregullave të sigurisë (8)

5. Malware që enkripton të dhënat dhe kërkon pagesë financiare për deshifrim (10)

7. Udhëzime të strukturuara si NIST që përdoren për menaxhimin e rreziqeve kibernetike (7)

Pika e kontrollit 5, alternativa: Çelësa të aksesueshëm të fjalëkryqit

Përdoruesit e lexuesve të ekranit dhe të tastierës mund t'i shkruajnë përgjigjet e fjalëkryqit drejtpërdrejt në fushat e tekstit më poshtë.

HORIZONTALISHT

2 horizontalisht: Eksploit i synuar para se shitësi të lëshojë një arnim (7 shkronja):

6 horizontalisht: Verifikim sigurie që kërkon dy ose më shumë faktorë autentikimi (14 shkronja):

8 horizontalisht: Praktikat më të mira për menaxhimin e kredencialeve dhe çelësave të autentikimit (8 shkronja):

VERTIKALISHT

1 vertikalisht: Sistem joshës i ngritur për të joshur dhe analizuar aktorët keqdashës (8 shkronja):

3 vertikalisht: Plan i strukturuar për trajtimin dhe zbutjen e shkeljeve të sigurisë (9 shkronja):

4 vertikalisht: Barrierë rrjeti që filtron trafikun sipas rregullave të sigurisë (8 shkronja):

5 vertikalisht: Malware që enkripton të dhënat dhe kërkon pagesë financiare për deshifrim (10 shkronja):

7 vertikalisht: Udhëzime të strukturuara si NIST që përdoren për menaxhimin e rreziqeve kibernetike (7 shkronja):

Pika e kontrollit 6: Kërkimi i fjalës së fshehur

Gjej 8 termat kyç të fjalorit të fshehur në rrjetën më poshtë. Fjalët mund të jenë horizontale, vertikale ose diagonale.

Z	E	R	O	D	A	Y	P	R	Z	T	C	Z	U	Ë
I	L	F	Z	Ç	L	D	Ë	P	X	H	O	C	T	B
E	L	A	Z	M	Ç	J	R	A	D	O	M	D	E	F
R	A	G	Ç	Q	P	K	G	D	G	N	Q	Z	R	E
A	W	P	U	E	A	A	J	P	N	E	L	O	S	X
W	E	P	I	Q	S	Q	I	Ç	L	Y	Y	B	Ë	Q
M	R	X	V	H	H	A	G	Q	Z	P	Y	Y	J	Ë
O	I	G	L	P	I	I	J	K	K	O	S	N	F	O
S	F	P	F	Z	G	A	E	N	U	T	Ë	T	C	Y
N	Q	Y	B	F	J	K	Z	Ë	I	M	O	M	V	C
A	M	U	L	T	I	F	A	K	T	O	R	I	A	L
R	K	Z	Y	Ë	E	Y	N	V	T	J	T	O	B	M
U	S	K	O	R	N	I	Z	Ë	K	F	T	Ç	Y	T
I	Q	B	V	Z	Ë	Y	K	Q	P	X	G	N	Ç	A
Ç	I	P	U	V	V	J	H	G	S	G	Ë	B	E	G

LISTA E FJALËVE TË LEKSIKUT

RANSOMWARE MULTIFAKTORIAL ZERODAY HONEYPOT FIREWALL PËRGJIGJE HIGJIENË KORNIZË

Pika e kontrollit 6, alternativa: Përputhja e aksesueshme e fjalorit

Përputh secilin nga 8 termat e fjalorit nga Kërkimi i fjalëve me përkufizimin e saktë të tij, duke shkruar shkronjën (A-H) në vendin bosh.

TERMA LEKSIKORË

- **A. RANSOMWARE**
- **B. MULTIFAKTORIAL**
- **C. ZERODAY**
- **D. HONEYPOT**
- **E. FIREWALL**
- **F. PËRGJIGJE**
- **G. HIGJIENË**
- **H. KORNIZË**

PËRKUFIZIME DHE FUSHA PËRPUTHJEJE

1. Barrierë rrjeti që filtron trafikun sipas rregullave të sigurisë.
2. Plan i strukturuar për trajtimin dhe zbutjen e shkeljeve të sigurisë.
3. Malware që enkripton të dhënat dhe kërkon pagesë financiare për deshifrim.
4. Verifikim sigurie që kërkon dy ose më shumë faktorë autentikimi.
5. Praktikat më të mira për menaxhimin e kredencialeve dhe çelësave të autentikimit.
6. Udhëzime të strukturuara si NIST që përdoren për menaxhimin e rreziqeve kibernetike.
7. Eksploit i synuar para se shitësi të lëshojë një arnim.
8. Sistem joshës i ngritur për të joshur dhe analizuar aktorët keqdashës.

Pika e kontrollit 7: Sfida e fjalëve të përzier

Rirenditi shkronjat më poshtë për të zbuluar konceptet dhe termat kryesorë të sigurisë kibernetike. Shkruaji përgjigjet në kutitë e dhëna.

1. RWMOARAESN
2. ZRYADOE
3. EIFWALLR
4. JNËEIHIG
5. OLIUKTILFRA MAT
6. OTEPHYON
7. IPJEGGËJR
8. ONËKZIR

Aktivitet bonus: Mendo shpejt

3 PËRGJIGJE PËR ÇDO KATEGORI. FITON KUSH E PLOTËSON I PARI LISTËN.

1	Punë në sigurinë kibernetike			
2	Arsye për të përditësuar softuerin			
3	Gjëra që mund të bllokojë një firewall			
4	Shenja paralajmëruese në një email			
5	Gjëra që ruan si kopje rezervë			
6	Lloje të njohura sulmesh kibernetike			
7	Gjëra që mund të joshë një honeypot			
8	Informacione që nuk duhet t'i ndash kurrë			
9	Shenja që një kompjuter është i infektuar			
10	Filma ose seriale për hakerët			
11	Shtresa sigurie që mund të ndërtosh			
12	Gjëra për t'u ushtruar në një stërvitje sigurie			
13	Mjete sigurie që njeh			
14	Njerëz që mund t'i pyesësh për ndihmë me IT-në			
15	Fjalë që fillojnë me 'kiber'			

Pika e kontrollit 8: Studime rasti për sigurinë kibernetike

Zbato konceptet që ke mësuar për të zgjidhur skenarët reale më poshtë.

STUDIMI I RASTIT 1: STRATEGJIA E RIKUPERIMIT NGA RANSOMWARE



Skenari: Një rrjet kompanie është infektuar me ransomware, i cili ka kyçur baza të dhënash kritike. Sulmuesit kërkojnë pagesë 100,000 dollarë në kriptovalutë. Kompania ka kopje rezervë offline nga 24 orë më parë.

Pyetje për diskutim: Analizo rreziqet e pagesës dhe vlerëso strategjinë e rimëkëmbjes.

STUDIMI I RASTIT 2: MBROJTJET KUNDËR CREDENTIAL STUFFING



Skenari: Një shërbim online përjeton një sulm credential stuffing, ku hakerët testojnë miliona çifte emër përdoruesi/fjalëkalim të vjedhura nga faqe të tjera.

Pyetje për diskutim: Përshkruaj në detaje mekanizmin e këtij sulmi dhe përshkruaj dy sisteme mbrojtjeje.

Pika e kontrollit 9: Deshifrimi i kodit

Një profesionist i sigurisë kibernetike mbron asetet e rrjetit nga aktorët e kërcënimeve online. Përdor çelësin shkronjë-numër më poshtë për të deshifruar mesazhin duke shkruar shkronjat përkatëse në hapësirat e zbrazëta.

ÇELËSI I ENKRIPTIMIT SHKRONJË-NË-NUMËR

A=1 B=2 C=3 Ç=4 D=5 E=6 Ë=7 F=8 G=9

H=10 I=11 J=12 K=13 L=14 M=15 N=16 O=17 P=18

Q=19 R=20 S=21 T=22 U=23 V=24 X=25 Y=26 Z=27

21	11	9	23	20	17	12	6		21	11	21	22	6	15	11	16		15	6
				1	23	22	6	16	22	11	13	11	15						
		15	23	14	22	11	8	1	13	22	17	20	11	1	14				

Mesazhi i deshifruar:

KËSHILLË: ÇDO NUMËR PËRFAQËSON POZICIONIN E ASAJ SHKRONJE NË ALFABET (P.SH. 1 = A, 2 = B, 27 = Z).

Pika e kontrollit 10: Pyetje të shpeshta bazë për sigurinë kibernetike (Pjesa A)

Rishiko pyetje dhe përgjigje të zakonshme për zbutjen e kërcënimeve në internet.

Q1: Cili është objektivi kryesor i sigurisë kibernetike?

Objektivi kryesor është mbrojtja e rrjeteve, pajisjeve dhe të dhënave nga qasja e paautorizuar, sulmet dhe dëmtimet aksidentale.

Q2: Si ndryshon phishing-u nga spear phishing?

Phishing-u është një fushatë e gjerë email-esh që synon përdorues të rastësishëm, ndërsa spear phishing synon individë të veçantë duke përdorur të dhëna të personalizuara.

Q3: Çfarë është një firewall rrjeti?

Një firewall është sistem sigurie i rrjetit që monitoron dhe filtron trafikun hyrës e dalës bazuar në rregulla të paracaktuara sigurie.

Q4: Pse është e nevojshme vërtetimi shumëfaktorësh (MFA)?

MFA shton një shtresë kritike mbrojtjeje, duke parandaluar aksesin edhe nëse sulmuesit vjedhin ose thyejnë kredencialet kryesore të fjalëkalimit.

Q5: Çfarë e përcakton një virus kompjuterik?

Një virus është malware vetëpërsëritës që ngjitet te skedarët e pastër dhe përhapet nëpër sisteme pasi ekzekutohet.

Pika e kontrollit 10: Pyetje të shpeshta bazë për sigurinë kibernetike (Pjesa B)

Rishiko pyetje dhe përgjigje të zakonshme për zbutjen e kërcënimeve në internet.

Q6: Si i bllokon ransomware të dhënat lokale?

Ransomware përdor algoritme kriptografike për t'i enkriptuar skedarët e përdoruesit, duke i bërë të palexueshëm derisa të zbatohet një çelës dekriptimi.

Q7: Çfarë është një cenueshmëri zero-day?

Një zero-day është një e metë sigurie në softuer e panjohur për shitësin, që nuk lë kohë për zhvillimin e patch-it para shfrytëzimit.

Q8: Cili është roli i kuadrit NIST?

Kuadri i NIST ofron udhëzime dhe standarde vullnetare për të ndihmuar organizatat të menaxhojnë dhe të zvogëlojnë rreziqet e sigurisë kibernetike.

Q9: Çfarë është një plan reagimi ndaj incidenteve të sigurisë?

Është një set i dokumentuar procedurash për zbulimin, përmbajtjen dhe rimëkëmbjen nga shkeljet e sigurisë dhe kompromentimi i rrjetit.

Q10: Si i shfrytëzon inxhinieria sociale përdoruesit?

Inxhinieria sociale përdor manipulim psikologjik për t'i nxitur punonjësit të zbulojnë fjalëkalime ose të shkarkojnë skedarë keqdashës.

Pika e kontrollit 10: Pyetje të shpeshta të avancuara për sigurinë (Pjesa C)

Eksploro aspektet e avancuara teknike të kornizave të sigurisë, analizës së malware-it dhe pajtueshmërisë me të dhënat.

Q1: Si i mbingarkon një sulm DDoS serverët e uebit?

Një sulm DDoS koordinon miliona pajisje botnet të kompromentuara për të përmbytur një server me trafik, duke shteruar kufijtë e gjerësisë së brezit dhe të CPU-së.

Q2: Cili është ndryshimi midis enkriptimit simetrik dhe asimetrik?

Enkriptimi simetrik përdor një çelës të vetëm për enkriptim dhe dekriptim, ndërsa enkriptimi asimetrik përdor një çift çelësash publik dhe privat.

Q3: Si i ekzekutojnë hakerët sulmet SQL injection?

Sulmuesit fusin komanda SQL keqdashëse në fushat e formularëve, duke mashtruar bazën e të dhënave në backend që të lëshojë regjistra përdoruesish të paautorizuar.

Q4: Çfarë është lëvizja anësore (lateral movement) në ndërhyrjet në rrjet?

Është teknika ku sulmuesit shfrytëzojnë qasjen fillestare në server për të kompromentuar sisteme të tjera të ndërlidhura në rrjetin e brendshëm.

Q5: Si e ridrejton DNS spoofing trafikun e uebit?

Falsifikimi i DNS ndryshon regjistrimet e memories së serverit të emrave, duke i drejtuar përdoruesit legjitimë te faqe interneti të rreme që duken si origjinalet në vend të domeneve të synuara.

Pika e kontrollit 10: Pyetje të shpeshta të avancuara për sigurinë (Pjesa D)

Eksploro aspektet e avancuara teknike të kornizave të sigurisë, analizës së malware-it dhe pajtueshmërisë me të dhënat.

Q6: Çfarë është një token sigurie harduerik?

Është një pajisje fizike (si YubiKey) që gjeneron prova autentikimi kriptografike, duke ofruar mbrojtje maksimale kundër phishing-ut në distancë.

Q7: Si i përdorin ekipet e sigurisë honeypot-et joshës?

Ekipet vendosin serverë joprodhues kurth për të zbuluar ndërhyrjet herët dhe për të analizuar modelet e sulmit të aktorëve të paautorizuar.

Q8: Cili është parimi i privilegjit më të vogël?

Është standardi i sigurisë që kufizon të drejtat e qasjes së përdoruesve në minimumin absolut të nevojshëm për të kryer rolet e tyre të punës.

Q9: Si i shfrytëzon lidhjet një sulm Man-in-the-Middle?

Një sulmues përgjon dhe ndryshon komunikimet mes dy pajisjeve në rrjete të pa enkriptuara, duke vjedhur token-ë sesionesh dhe kredenciale.

Q10: Çfarë janë treguesit e kompromentimit (IOC)?

IOC-të janë tregues forensikë të dhënash, si modifikime të pazakonta të regjistrit ose trafik IP i dyshimtë, që tregojnë se një sistem është thyer.

Pjesa 11: 10 fakte dhe njohuri nga bota reale për sigurinë kibernetike

Rishiko fakte reale për shkeljet e sigurisë, mekanizmat e mbrojtjes dhe standardet e pajtueshmërisë.

1. PERSPEKTIVË PËR SIGURINË

Sulmuesit skanojnë vazhdimisht internetin për serverë të cenueshëm dhe u dërgojnë emaile phishing kutive postare të punonjësve.

2. PERSPEKTIVË PËR SIGURINË

Gabimi njerëzor, si klikimi i lidhjeve phishing, është një faktor i zakonshëm në shkeljet e të dhënave, prandaj trajnimi ka rëndësi.

3. PERSPEKTIVË PËR SIGURINË

Kostot e një shkeljeje të të dhënave përfshijnë gjoba ligjore, humbjen e klientëve, hetimin dhe riparimin, dhe mund të arrijnë miliona dollarë.

4. PERSPEKTIVË PËR SIGURINË

MFA rezistente ndaj phishing-ut, si çelësat fizikë të sigurisë, është lloji më i fortë i MFA-së dhe standardi që CISA e nxit. [2]

5. PERSPEKTIVË PËR SIGURINË

Ransomware mbetet një kërcënim i madh për rrjetet e ndërmarrjeve, dhe CISA bën thirrje për kopjeruajtje offline të enkriptuara si mbrojtje kryesore. [4]

6. PERSPEKTIVË PËR SIGURINË

NIST Cybersecurity Framework 2.0 (2024) ka gjashtë funksione kryesore: Govern, Identify, Protect, Detect, Respond, Recover. [1]

7. NJOHURI PËR SIGURINË

Bot-et e credential stuffing testojnë në shkallë të gjerë çifte të rrjedhura emrash përdoruesi dhe fjalëkalimesh kundër portaleve të hyrjes së bankave dhe e-commerce.

8. NJOHURI PËR SIGURINË

Tregje shfrytëzimesh zero-day ekzistojnë në mbarë botën, ku cenueshmëri me ashpërsi të lartë mund të shiten për shuma të mëdha para se të korrigjohen.

9. NJOHURI PËR SIGURINË

Një sistem honeypot si karth lajmëron menjëherë për ndërhyrje, pasi përdoruesit legjitimë nuk kanë arsye ta përdorin.

10. PERSPEKTIVË PËR SIGURINË

Transport Layer Security (TLS) enkripton seancat e shfletuesit, duke parandaluar përgjimin e paketave në rrjetet publike Wi-Fi.

Referenca teknike dhe burime

Udhëzuesi i studimit dhe enigmat interaktive janë përpiluar nga standardet globale të NIST, OWASP dhe të pajtueshmërisë me privatësinë e të dhënave.

REFERENCA AKADEMIKE DHE TË INDUSTRISË

[1] NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[2] CISA. (n.d.). More than a Password.
https://www.cisa.gov/MFA

[3] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

[4] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[5] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[6] NIST. (2025). SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.
https://csrc.nist.gov/pubs/sp/800/61/r3/final

[7] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[8] OWASP. (n.d.). SQL Injection.
https://owasp.org/www-community/attacks/SQL_Injection

Çelësi i përgjigjeve: Pika e kontrollit 1 - Zgjedhje e shumëfishtë

1 **Sulmet phishing** PHISHING — Përgjigjja e saktë: A

SHËNIM PËR MËSUESIN

Fushatat phishing përpiqen të vjedhin kredencialet dhe të dhënat e ndjeshme të përdoruesve duke përdorur email-e të falsifikuara. Citim: OWASP Secure Configuration.

2 **Mbrojtja e llogarisë** ÇELËSI MFA — Përgjigjja e saktë: A

SHËNIM PËR MËSUESIN

Autentikimi me shumë faktorë (MFA) që përdor token-ë harduerikë ofron mbrojtjen më të fortë të aksesit në llogari. Citim: NIST Digital Identity.

3 **Kërcënimi i ransomware** RANSOMWARE — Përgjigjja e saktë: A

SHËNIM PËR MËSUESIN

Ransomware enkripton sisteme dhe të dhëna kritike, duke kërkuar pagesë me kriptovalutë për çelësat e dekriptimit. Citim: Center for Internet Security (CIS).

4 **Cenueshmëria zero-day** ZERO-DAY — Përgjigjja e saktë: A

SHËNIM PËR MËSUESIN

Kërcënimet zero-day shfrytëzojnë të meta sigurie të pakorrigjuara dhe të panjohura para se të bëhet i disponueshëm një korrigjim nga shitësi. Citim: OWASP Secure Configuration.

5 **Kornizat e sigurisë** KORNIZA — Përgjigjja e saktë: A

SHËNIM PËR MËSUESIN

Kornizat si NIST ofrojnë udhëzime të strukturuara për të ndihmuar organizatat të menaxhojnë dhe të zvogëlojnë rreziqet kibernetike. Citim: NIST Digital Identity.

Çelësi i përgjigjeve: Pika e kontrollit 2 - E vërtetë ose e gabuar

6 **Phishing i synuar** PHISHING — **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

Sulmet phishing synojnë si rrjetet korporative, ashtu edhe llogaritë personale për të zgjeruar vektorët e shfrytëzimit. Citim: OWASP Secure Configuration.

7 **Pyetja 7** — **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

MFA kërkon një faktor të dytë, ndaj një fjalëkalim i vjedhur vetëm zakonisht nuk mjafton për t'u identifikuar.

8 **Firewall-i i trafikut** FIREWALL — **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

Firewall-et inspektojnë dhe bllokojnë trafikun në porta specifike të rrjetit për të filtruar lidhjet e paautorizuara. Citim: Center for Internet Security (CIS).

9 **Reagimi ndaj zero-day** ZERO-DAY — **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

Korrigjimi i të metave zero-day kërkon korrigjime kodi dhe filtrim WAF, pasi nënshkrimet nuk ekzistojnë ende. Citim: OWASP Secure Configuration.

10 **Honeypot-e joshëse** HONEYPOT — **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

Honeypot-et janë serverë mashtrues që përdoren nga ekipet e sigurisë për të joshur, alarmuar dhe studiuar aktorët keqdashës. Citim: Center for Internet Security (CIS).

Çelësat e fjalorit dhe rubrika e vlerësimit

Rubrika e vlerësimit për mësuesin: Jep 1 pikë për çdo përputhje të saktë (8 pikë gjithsej) dhe term konteksti (6 pikë gjithsej).

PIKA E KONTROLLIT 4: ÇELËSI – PËRPUTHJA E KONCEPTEVE

D 1. Kërcënimi i ransomware-it	G 2. Autentikim shumëfaktorësh	E 3. Shfrytëzim zero-day	H 4. Honeypot joshës
C 5. Firewall kundër ndërhyrjeve	B 6. Reagimi ndaj incidenteve	F 7. Higjiena e fjalëkalimeve	A 8. Kornizë sigurie

PIKA E KONTROLLIT 3: ÇELËSI – TERMAT KRYESORË

1 FIREWALL	2 EKSPLOIT	3 PHISHING	4 MALWARE
5 HIGJIENË	6 ENKRIPTIM		

PIKA E KONTROLLIT 6, ALTERNATIVA: ÇELËSI – PËRPUTHJA E FJALËVE

1 E – FIREWALL	2 F – PËRGJIGJE	3 A – RANSOMWARE	4 B – MULTIFAKTORIAL
5 G – HIGJIENË	6 H – KORNIZË	7 C – ZERODAY	8 D – HONEYPOT

SHËNIME PËR DISKUTIM PËR MËSUESIT

Termat kryesorë:
Kontrollo nëse nxënësit mund të shpjegojnë Kërcënimi i ransomware-it, Autentikim shumëfaktorësh dhe Shfrytëzim zero-day me fjalët e tyre dhe të japin një shembull për secilin.

Studimet e rastit:
Kërkoju nxënësve t'i mbështesin rekomandimet me fakte nga fleta, jo me supozime.

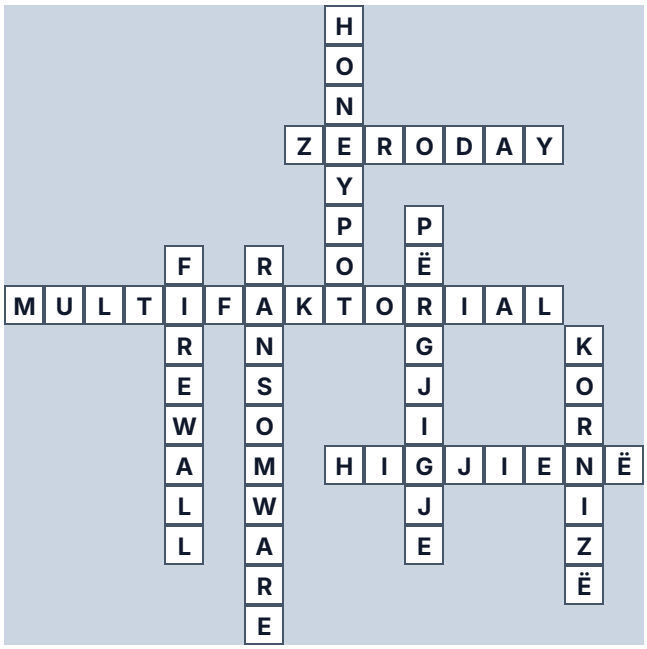
Vlerësimi i burimeve:
Kërkoju nxënësve të verifikojnë të paktën një pohim në burimet e fletës dhe diskutoni pse numrat, çmimet dhe rregullat mund të ndryshojnë me kalimin e kohës.

Çelësat e enigmave dhe shënimet për mësuesin

ZGJIDHJA E LOJËS ME FJALË

Z	E	R	O	D	A	Y	P	R	Z	T	C	Z	U	Ë
I	L	F	Z	Ç	L	D	Ë	P	X	H	O	C	T	B
E	L	A	Z	M	Ç	J	R	A	D	O	M	D	E	F
R	A	G	Ç	Q	P	K	G	D	G	N	Q	Z	R	E
A	W	P	U	E	A	A	J	P	N	E	L	O	S	X
W	E	P	I	Q	S	Q	I	Ç	L	Y	Y	B	Ë	Q
M	R	X	V	H	H	A	G	Q	Z	P	Y	Y	J	Ë
O	I	G	L	P	I	I	J	K	K	O	S	N	F	O
S	F	P	F	Z	G	A	E	N	U	T	Ë	T	C	Y
N	Q	Y	B	F	J	K	Z	Ë	I	M	O	M	V	C
A	M	U	L	T	I	F	A	K	T	O	R	I	A	L
R	K	Z	Y	Ë	E	Y	N	V	T	J	T	O	B	M
U	S	K	O	R	N	I	Z	Ë	K	F	T	Ç	Y	T
I	Q	B	V	Z	Ë	Y	K	Q	P	X	G	N	Ç	A
Ç	I	P	U	V	V	J	H	G	S	G	Ë	B	E	G

ZGJIDHJA E FJALËKRYQIT



UDHËZUES PËR MËSUESIN PËR ZGJIDHJET E KRYQËZËS

HORIZONTALISHT

2 horizontalisht: ZERODAY Eksploit i synuar para se shitësi të lëshojë një arnim (7 shkronja)

6 horizontalisht: MULTIFAKTORIAL Verifikim sigurie që kërkon dy ose më shumë faktorë autentikimi (14 shkronja)

8 horizontalisht: HIGJIENË Praktikat më të mira për menaxhimin e kredencialeve dhe çelësave të autentikimit (8 shkronja)

VERTIKALISHT

1 vertikalisht: HONEYPOT Sistem joshës i ngritur për të joshur dhe analizuar aktorët keqdashës (8 shkronja)

3 vertikalisht: PËRGJIGJE Plan i strukturuar për trajtimin dhe zbutjen e shkeljeve të sigurisë (9 shkronja)

4 vertikalisht: FIREWALL Barrierë rrjeti që filtron trafikun sipas rregullave të sigurisë (8 shkronja)

5 vertikalisht: RANSOMWARE Malware që enkripton të dhënat dhe kërkon pagesë financiare për deshifrim (10 shkronja)

7 vertikalisht: KORNIZË Udhëzime të strukturuara si NIST që përdoren për menaxhimin e rreziqeve kibernetike (7 shkronja)

Çelësi i fjalëve të përzierura dhe i zgjidhjes së kodit

Çelësi i vlerësimit për aktivitetin e rirenditjes së fjalorit dhe për Sfidën e Kodit të Fshehtë.

ÇELËSI I RIRENDITJES SË FJALËVE

1. RWMOARAESN — **RANSOMWARE**
2. ZRYADOE — **ZERODAY**
3. EIFWALLR — **FIREWALL**
4. JNËEIHIG — **HIGJIENË**
5. OLIUKTILFRAMAT — **MULTIFAKTORIAL**
6. OTEPHYON — **HONEYPOT**
7. IPJEGGËJR — **PËRGJIGJE**
8. ONËKZIR — **KORNIZË**

ÇELËSI I SFIDËS SË KODIT TË FSHEHTË

"SIGUROJE SISTEMIN ME AUTENTIKIM MULTIFAKTORIAL"

Çelësi i studimeve të rastit

A Studimi i rastit 1: Strategjia e rikuperimit nga ransomware

Zgjidhja për mësuesin

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Analiza e skenarit: Një rrjet korporativ është infektuar me ransomware, që ka kyçur bazat kritike të të dhënave. Sulmuesit kërkojnë një pagesë prej $100,000 në kriptovalutë. Kompania ka kopje rezervë offline nga 24 orë më parë.
- Strategjia dhe zgjidhja e rekomanduar: Rreziqet e pagesës: Pagesa nuk garanton deshifrimin e skedarëve, e etiketon kompaninë si objektiv që paguan dhe financon veprimtari kriminale. Strategjia e rimëkëmbjes: Ekipi duhet të izolojë hostet e infektuar, të fshijë serverët e kompromet uar dhe të rikthejë të dhënat nga kopjet rezervë offline. Duhet të korrigjojë vektorin fillestar të qasjes (phishing ose shfrytëzim) për të parandaluar riinfektimin e menjëhershëm.

B Studimi i rastit 2: Mbrojtjet kundër credential stuffing

Zgjidhja për mësuesin

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Analiza e skenarit: Një shërbim online përjeton një sulm credential stuffing, ku hakerët testojnë miliona çifte emër përdoruesi/fjalëkalim të vjedhura nga faqe të tjera.
- Strategjia dhe zgjidhja e rekomanduar: Mekanizmi: Sulmuesit shfrytëzojnë ripërdorimin e fjalëkalimeve nëpër faqe duke përdorur robotë të automatizuar për t'u identifikuar në llogaritë e përdoruesve. Mbrojtjet: 1. Vërtetimi shumëfaktorësh (MFA) bllokon përpjekjet për hyrje edhe nëse fjalëkalimi është i saktë. 2. Vendosja e kufizimit të shpejtësisë dhe CAPTCHA-ve bllokon trafikun e robotëve të automatizuar që mbyt pikat e hyrjes.